EC-Council

C|EH™

Certified Ethical Hacker

Ethical Hacking and Countermeasures v11

Professional Series

EC-COUNCIL OFFICIAL CURRICULA

Ethical Hacking and Countermeasures

Version 11

EC-Council

Copyright © 2020 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures to ensure that the content is current and accurate; however, because of the possibility of human or mechanical error, we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions nor for the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject-matter experts from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license or contract, you may notify us at **legal@eccouncil.org**. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions, and inaccuracies to EC-Council at **legal@eccouncil.org**. If you have any issues, please contact us at **support@eccouncil.org**.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Foreword

Since you are reading this CEHv11 courseware, you most likely realize the importance of information systems security. However, we would like to put forth our motive behind compiling a resource such as this one and what you can gain from this course.

You might find yourself asking what sets this course apart from the others out there. The truth is that no single courseware can address all the issues of information security in a detailed manner. Moreover, the rate at which exploits, tools, and methods are being discovered by the security community makes it difficult for one program to cover all the necessary facets of information security. This doesn't mean that this course is inadequate in any way as we have worked to cover all major domains in such a manner that the reader will be able to appreciate the way security has evolved over time as well as gain insight in to the fundamental workings relevant to each domain. It is a blend of academic and practical wisdom supplemented with tools that the reader can readily access in order to obtain a hands-on experience.

The emphasis throughout the courseware is on gaining practical know-how, which explains the stress on free and accessible tools. You will read about some of the most widespread attacks seen, the popular tools used by attackers, and how attacks have been carried out using ordinary resources.

You may also want to know what to expect once you have completed the course. This courseware is a resource material. Any penetration tester can tell you that there is no one straight methodology or sequence of steps that you can follow while auditing a client site. There is no one template that will meet all your needs. Your testing strategy will vary with the client, the basic information about the system or situation, and the resources at your disposal. However, for each stage you choose – be it enumeration, firewall, penetration of other domains - you will find something in this courseware that you can definitely use.

Finally, this is not the end! This courseware is to be considered a constant work-in-progress because we will be adding value to this courseware over time. You may find some aspects extremely detailed, while others may have less detail. We are constantly asking ourselves if the content helps explain the core point of the lesson, and we constant calibrate our material with that in mind. We would love to hear your viewpoints and suggestions so please send us your feedback to help in our quest to constantly improve our courseware.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

About the EC-Council CEH Program

If you want to stop hackers from invading your network, first you've got to invade their minds.

Computers around the world are systematically being victimized by rampant hacking. This hacking is not only widespread, but is being executed so flawlessly that the attackers compromise a system, steal everything of value and completely erase their tracks.

The goal of the ethical hacker is to help the organization take preemptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits. This philosophy stems from the proven practice of trying to catch a thief, by thinking like a thief. As technology advances and organization depend on technology increasingly, information assets have evolved into critical components of survival.

If hacking involves creativity and thinking 'out-of-the-box', then vulnerability testing and security audits will not ensure the security proofing of an organization. To ensure that organizations have adequately protected their information assets, they must adopt the approach of 'defense in depth'. In other words, they must penetrate their networks and assess the security posture for vulnerabilities and exposure.

The Ethical Hacker is an individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods as a Hacker. Hacking is a felony in some countries. When it is done by request and under a contract between an Ethical Hacker and an organization, it is legal. The most important point is that an Ethical Hacker has authorization to probe the target.

The CEH Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.

To achieve the Certified Ethical Hacker Certification, you must pass the CEH exam 312-50.

Please visit **https://www.eccouncil.org/programs/certified-ethical-hacker-ceh** for more information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization composed of industry and subject matter experts working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the Certified Ethical Hacker (C|EH) program with the goal of teaching the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge of hundreds of subject-matter experts, the CEH program has rapidly gained popularity around the world and is now delivered in more than 145 countries by more than 950 authorized training centers. It is considered as the benchmark for many government entities and major corporations around the globe.

EC-Council, through its impressive network of professionals and huge industry following, has also developed a range of other leading programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are tightening security networks around the world and beating hackers at their own game.

Other EC-Council Programs

Security Awareness: Certified Secure Computer User

C|SCU
Certified Secure Computer User

The purpose of the CSCU training program is to provide students with the necessary knowledge and skills to protect their information assets. This class will immerse students in an interactive learning environment where they will acquire fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, viruses and backdoors, email hoaxes, sexual predators and other online threats, loss of confidential information, hacking attacks, and social engineering. More importantly, the skills learnt from the class help students take the necessary steps to mitigate their security exposure.

Network Defense: Certified Network Defender

C|ND
Certified Network Defender

Students enrolled in the Certified Network Defender course will gain a detailed understanding of network defense and develop their hands-on expertise to perform in real-life network defense situations. They will gain the depth of technical knowledge required to actively design a secure network within your organization. This course provides a fundamental understanding of the true nature of data transfer, network technologies, and software technologies so that students may understand how networks operate, how automation software behaves, and how to analyze networks and their defense.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Students will learn how to protect, detect, and respond to the network attacks as well as learning about network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration. Students will also learn the intricacies of network traffic signature, analysis, and vulnerability scanning, which will help in designing improved network security policies and successful incident response plans. These skills will help organizations foster resiliency and operational continuity during attacks.

Penetration Testing: Certified Penetration Testing Professional

CPENT certification requires you to demonstrate the application of advanced penetration testing techniques such as advanced Windows attacks, IOT systems attacks, advanced binaries exploitation, exploits writing, bypassing a filtered network, Operational Technology (OT) pen testing, accessing hidden networks with pivoting and double pivoting, privilege escalation, and evading defense mechanisms.

EC-Council's CPENT standardizes the knowledge base for penetration testing professionals by incorporating best practices followed by experienced experts in the field. The objective of the CPENT is to ensure that each professional follows a strict code of ethics, is exposed to the best practices in the domain of penetration testing and aware of all the compliance requirements required by the industry.

Unlike a normal security certification, the CPENT credential provides an assurance that security professionals possess skills to analyze the security posture of a network exhaustively and recommend corrective measures authoritatively. For many years EC-Council has been certifying IT Security Professionals around the globe to ensure these professionals are proficient in network security defense mechanisms. EC-Council's credentials vouch for their professionalism and expertise thereby making these professionals more sought after by organizations and consulting firms globally.

Computer Forensics: Computer Hacking Forensic Investigator

Computer Hacking Forensic Investigator (CHFI) is a comprehensive course covering major forensic investigation scenarios. It enables students to acquire crucial hands-on experience with various forensic investigation techniques. Students learn how to utilize standard forensic tools to successfully carry out a computer forensic investigation, preparing them to better aid in the prosecution of perpetrators.

EC-Council's CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification bolsters the applied knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of network infrastructures.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Handling: EC-Council Certified Incident Handler

EC-Council's Certified Incident Handler (E|CIH) program has been designed and developed in collaboration with cybersecurity and incident handling and response practitioners across the globe. It is a comprehensive specialist-level program that imparts knowledge and skills that organizations need to effectively handle post breach consequences by reducing the impact of the incident, from both a financial and a reputational perspective.

E|CIH is a method-driven program that uses a holistic approach to cover vast concepts concerning organizational incident handling and response from preparing and planning the incident handling response process to recovering organizational assets after a security incident. These concepts are essential for handling and responding to security incidents to protect organizations from future threats or attacks.

Management: Certified Chief Information Security Officer

The Certified Chief Information Security Officer (CCISO) program was developed by EC-Council to fill a knowledge gap in the information security industry. Most information security certifications focus on specific tools or practitioner capabilities. When the CCISO program was developed, no certification existed to recognize the knowledge, skills, and aptitudes required for an experienced information security professional to perform the duties of a CISO effectively and competently. In fact, at that time, many questions existed about what a CISO really was and the value this role adds to an organization.

The CCISO Body of Knowledge helps to define the role of the CISO and clearly outline the contributions this person makes in an organization. EC-Council enhances this information through training opportunities conducted as instructor-led or self-study modules to ensure candidates have a complete understanding of the role. EC-Council evaluates the knowledge of CCISO candidates with a rigorous exam that tests their competence across five domains with which a seasoned security leader should be familiar.

Application Security: Certified Application Security Engineer

The Certified Application Security Engineer (CASE) credential is developed in partnership with large application and software development experts globally. The CASE credential tests the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices in today's insecure operating environment.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The CASE certified training program is developed concurrently to prepare software professionals with the necessary capabilities that are expected by employers and academia globally.It is designed to be a hands-on, comprehensive application security course that will help software professionals create secure applications. The training program encompasses security activities involved in all phases of the Software Development Lifecycle (SDLC): planning, creating, testing, and deploying an application.

Unlike other application security trainings, CASE goes beyond just the guidelines on secure coding practices and includes secure requirement gathering, robust application design, and handling security issues in post development phases of application development. This makes CASE one of the most comprehensive certifications on the market today. It is desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

Incident Handling: Certified Threat Intelligence Analyst

C|TIA
Certified Threat Intelligence Analyst

Certified Threat Intelligence Analyst (C|TIA) is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and mitigate business risks by converting unknown internal and external threats into known threats. It is a comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence.

In the ever-changing threat landscape, C|TIA is an essential Threat Intelligence training program for those who deal with cyber threats on a daily basis. Organizations today demand a professional-level cybersecurity threat intelligence analyst who can extract the intelligence from data by implementing various advanced strategies. Such professional-level Threat Intelligence training programs can only be achieved when the core of the curricula maps with and is compliant to government and industry published threat intelligence frameworks.

Incident Handling: Certified SOC Analyst

C|SA™
Certified SOC Analyst

The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CEH Exam Information

CEH Exam Details	
Exam Title	**Certified Ethical Hacker (CEH)**
Exam Code	**312-50**
Availability	**EC-Council Exam Portal** (please visit **https://www.eccexam.com**) **VUE** (please visit **https://home.pearsonvue.com/eccouncil**)
Duration	**4 Hours**
Questions	**125**
Passing Score	Please refer **https://cert.eccouncil.org/faq.html**

Please visit **https://cert.eccouncil.org/certified-ethical-hacker.html** for more information.

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Table of Contents

Module 01: Introduction to Ethical Hacking **1**

Information Security Overview 3

Cyber Kill Chain Concepts 12

Hacking Concepts 27

Ethical Hacking Concepts 38

Information Security Controls 47

Information Security Laws and Standards 76

Module 02: Footprinting and Reconnaissance **92**

Footprinting Concepts 94

Footprinting through Search Engines 101

Footprinting through Web Services 121

Footprinting through Social Networking Sites 162

Website Footprinting 172

Email Footprinting 192

Whois Footprinting 197

DNS Footprinting 203

Network Footprinting 208

Footprinting through Social Engineering 219

Footprinting Tools 222

Footprinting Countermeasures 232

Module 03: Scanning Networks **236**

Network Scanning Concepts 238

Scanning Tools 245

Host Discovery 259

Port and Service Discovery 277

OS Discovery (Banner Grabbing/OS Fingerprinting) 320

Scanning Beyond IDS and Firewall 335

Draw Network Diagrams 382

Module 04: Enumeration **390**

Enumeration Concepts 392

NetBIOS Enumeration 401

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SNMP Enumeration 413
LDAP Enumeration 421
NTP and NFS Enumeration 425
SMTP and DNS Enumeration 438
Other Enumeration Techniques 454
Enumeration Countermeasures 476

Module 05: Vulnerability Analysis 482
Vulnerability Assessment Concepts 485
Vulnerability Classification and Assessment Types 506
Vulnerability Assessment Solutions and Tools 515
Vulnerability Assessment Reports 538

Module 06: System Hacking 544
System Hacking Concepts 546
Gaining Access 552
Escalating Privileges 651
Maintaining Access 693
Clearing Logs 800

Module 07: Malware Threats 835
Malware Concepts 837
APT Concepts 848
Trojan Concepts 856
Virus and Worm Concepts 907
Fileless Malware Concepts 949
Malware Analysis 970
Countermeasures 1059
Anti-Malware Software 1066

Module 08: Sniffing 1076
Sniffing Concepts 1078
Sniffing Technique: MAC Attacks 1097
Sniffing Technique: DHCP Attacks 1112
Sniffing Technique: ARP Poisoning 1124
Sniffing Technique: Spoofing Attacks 1140

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Technique: DNS Poisoning 1158
Sniffing Tools 1171
Countermeasures 1185
Sniffing Detection Techniques 1188

Module 09: Social Engineering 1197
Social Engineering Concepts 1199
Social Engineering Techniques 1207
Insider Threats 1236
Impersonation on Social Networking Sites 1244
Identity Theft 1250
Countermeasures 1257

Module 10: Denial-of-Service 1280
DoS/DDoS Concepts 1282
DoS/DDoS Attack Techniques 1287
Botnets 1313
DDoS Case Study 1325
DoS/DDoS Attack Tools 1334
Countermeasures 1340
DoS/DDoS Protection Tools 1362

Module 11: Session Hijacking 1371
Session Hijacking Concepts 1373
Application Level Session Hijacking 1389
Network Level Session Hijacking 1416
Session Hijacking Tools 1426
Countermeasures 1431

Module 12: Evading IDS, Firewalls, and Honeypots 1457
IDS, IPS, Firewall, and Honeypot Concepts 1459
IDS, IPS, Firewall, and Honeypot Solutions 1501
Evading IDS 1525
Evading Firewalls 1549
IDS/Firewall Evading Tools 1578
Detecting Honeypots 1582

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IDS/Firewall Evasion Countermeasures 1589

Module 13: Hacking Web Servers 1593
Web Server Concepts 1595
Web Server Attacks 1605
Web Server Attack Methodology 1630
Web Server Attack Tools 1663
Countermeasures 1673
Patch Management 1689
Web Server Security Tools 1696

Module 14: Hacking Web Applications 1710
Web Application Concepts 1713
Web Application Threats 1725
Web Application Hacking Methodology 1805
Web API, Webhooks, and Web Shell 1901
Web Application Security 1954

Module 15: SQL Injection 1997
SQL Injection Concepts 1999
Types of SQL Injection 2014
SQL Injection Methodology 2031
SQL Injection Tools 2114
Evasion Techniques 2121
Countermeasures 2139

Module 16: Hacking Wireless Networks 2161
Wireless Concepts 2163
Wireless Encryption 2180
Wireless Threats 2198
Wireless Hacking Methodology 2228
Wireless Hacking Tools 2311
Bluetooth Hacking 2325
Countermeasures 2339
Wireless Security Tools 2352

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module 17: Hacking Mobile Platforms **2370**
Mobile Platform Attack Vectors 2372
Hacking Android OS 2404
Hacking iOS 2460
Mobile Device Management 2493
Mobile Security Guidelines and Tools 2507

Module 18: IoT and OT Hacking **2536**
IoT Concepts 2539
IoT Attacks 2561
IoT Hacking Methodology 2607
IoT Hacking Tools 2649
Countermeasures 2661
OT Concepts 2675
OT Attacks 2704
OT Hacking Methodology 2730
OT Hacking Tools 2766
Countermeasures 2773

Module 19: Cloud Computing **2788**
Cloud Computing Concepts 2791
Container Technology 2818
Serverless Computing 2844
Cloud Computing Threats 2851
Cloud Hacking 2900
Cloud Security 2954

Module 20: Cryptography **2999**
Cryptography Concepts 3001
Encryption Algorithms 3008
Cryptography Tools 3045
Public Key Infrastructure (PKI) 3055
Email Encryption 3063
Disk Encryption 3084
Cryptanalysis 3090
Countermeasures 3118

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Glossary 3123
References 3148
Appendix A - Ethical Hacking Essential Concepts - I 3204
Appendix B - Ethical Hacking Essential Concepts - II 3322

Ethical Hacking and Countermeasures Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.